Business Purpose	• Company X desires to lower the response time from employees when a security breach occurs. • After building awareness to the types of security breaches employees may encounter and training employees on the process to responding to security breaches, incident response time will be lowered to five minutes or less.
Target Audience	• Any employee of company X that has access to confidential information such as Personal Identifiable Information (PII), Sensitive Personal Identifiable Information (SPII), Controlled Unclassified Information (CUII)
Training Time	20 minutes
Training Recommendation	• 1 e-Learning course • Final evaluation that confirms the learner understand the security breach reporting process

Deliverables	• 1 e-Learning course
	  ○ Developed in Articulate Storyline
	  ○ Includes voice-over narration
	• Job Aid: Steps to Incident Response

Learning Objectives	• Identify the most common types of security incidents • List in order the process of responding to security incidents

Training Outline	▪ Introduction
	  ○ Title of Course
	  ○ Navigation Tutorial
	▪ Define: What is an Incident?
	  ○ Violation of Acceptable Use Policies
	  ○ Violation of Standard Security Policies
	  ○ Violation of Security of Computer Use Policies
	  ○ (NOTE: We are assuming that employees are familiar with these policies. If policies need to be introduced more information will be needed.)
	▪ Explain: What are the types of incidents?
	  ○ 4 Types of incidents will be given
	  ○ Learner will review each type of incident that needs to be reported

- Type 1: equipment, media, and documents that are lost, damaged, or stolen
- Type 2: sending confidential reports to unauthorized viewers
- Type 3: allowing unauthorized persons to use your computer or credentials
- Type 4 viruses, phishing emails, and social engineering attacks that compromise information systems

- Knowledge Check
  - 2 questions given
  - Questions will be scenario based and require the learner to think about how they should respond to each situation
  - 2 attempts will be given with an explanation of why the answer is correct or incorrect

- Learn the process: How should I respond?
  - Four steps to reporting will be introduced:
    - Stop
    - Call
    - Email
    - Write
  - Detailed information about each step will be given.

- When can I resume working?
  - Voice narration will inform learner when they can resume working after a security incident has occurred.

- Summary
  - Types of incidents will be reviewed with a bulleted list
  - After types are reviewed, markers will appear on the image. There will be five markers, one will be an arrow while the rest will be numbers. These markers will review the steps to take to respond to security breach incidents.
    - Arrow- Time
    - Marker 1- Stop
    - Marker 2- Call
    - Marker 3- Email
    - Marker 4- Write
- Introduction to the Assessment
- Assessment
- Results
- Thank you for completing!

Evaluation Plan	▪ Knowledge Check o 2 Scenario based questions to assess knowledge of when to report a security incident. ▪ Assessment will be introduced to the learner o Quiz Questions with different response types o Quiz will cover learners' knowledge of how to respond to an incident o Learner needs 100% correct to pass